# A Review –Different Attacks in VANET for Various Traffic Area

**Urmila Prajapati[1] Pallavi Pahadiya[2]**
[1,2]Department of Electronics & Communication Engineering
[1,2]SIRT, Indore, India

*Abstract*— In the advancement of savvy urban communities over the world VANET assumes a crucial part for upgraded route amongst source and destination. The VANETs depends on infrastructure less organizes. It encourages vehicles to give data about security through vehicle to vehicle communication (V2V) or vehicle to infrastructure communication (V2I). In VANETs wireless communication between vehicles so attackers violate legitimacy, secrecy and security properties which additionally impact security. The VANET innovation is circled with security challenges nowadays. This review paper presents outline on VANETs engineering, a related overview on VANET with significant worry of the security issues. Further, counteractive action measures of those issues; furthermore, relative survey is finished. From the study, discovered that encryption and validation assumes a critical part in VANETS likewise some exploration heading characterized for future work.

***Key words:*** VANET, Routing Protocol, Infrastructure, Communication, Network Security and NS-2.35

## I. INTRODUCTION

VANETs are special case of ad hoc networks that the communicating entities are vehicles, and have unfixed or no infrastructure. VANETs are emerged for providing comfort and flexible services and information for passengers along their way like informing them about an emergency case after certain kilometers from their position. VANETs have different applications which can be applied by Peer-to-Peer (P2P) communication or via multi-hop communication. VANETs are called Inter-Vehicle Communications (IVC) or Vehicle-to-Vehicle communications (V2V); its applications are like cooperative traffic monitoring, optimization of a route to a destination, collision prevention, weather forecasting, and broadcasting information like advertisements for some goods, commodity and online services. This variety of applications leads to call these networks Intelligent Transportation System (ITS) [1,2]. Some problems in ad hoc networks which appear in VANETs communications like interference that can be produced from more than one node communicate to one node by a direct connection. So, the multi-hop connection is used with some technologies such as Bluetooth and frequency hopping [3]. But, due to the multi-hop transmission in VANETs, routing problems will exist greatly since no figure for a network infrastructure with vehicle entities.

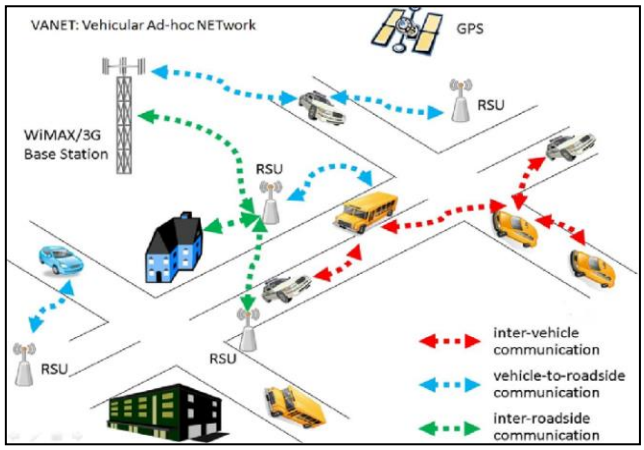


Fig. 1: VANET Infrastructure

VANETs are considered a subclass of MANETs (Mobile Ad Hoc Networks); but there some differences like topology change frequently with high speeds, high probability of network fragmentation since there are speedy vehicles, no strict limitations of power consumption, operation at large scales inside cities and their edges and high ways, and depending on vehicles behaviors in response or reaction for delivered messages [2]. Vehicles have specific units which make them communicate with other vehicles. These units are called On-Board Units (OBUs). In addition, the architecture of VANETs can take different styles which are cellular/WLAN (Wireless Local Area Network), ad hoc, and hybrid. For the first architecture, the vehicles receive and exchange data with base stations (also know by Road-Side Units (RSUs)) or fixed remote entities (V2R Communications). In the second one, the vehicles exchange messages directly together without intermediate entities (V2V communications).

## II. SECURITY ISSUES IN VANET

Security in VANET is a challenging problem for researchers in the era of cyber threats. The message passing from one vehicle to another vehicle may be hacked by an intruder who creates vulnerability in the systems performance [7], [8]. In this section, security challenges, security requirements, attackers on VANETs and various attacks in the VANET are studied.

### *A. Security Challenges in VANET*

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges:

*1) Real time Constraint:*

Most of the applications in VANET require time critical messages, like collision avoidance, hazard warning and accident warning information etc. Hence strict deadlines for the delivery of messages must be met.

Data Consistency Liability: In VANET even authenticate node can perform malicious activities that can cause

 

accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency.

*2) High Mobility and Volatility:*

Computational capability and energy supply in VANET is nearly same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that wired network produces.

Location Awareness: The increased reliance of VANET on GPS or other specific location based instruments may affect its applications in case of occurrence of any error.

*3) Tradeoff between authentication and privacy:*

For the authentication of the messages that are to be transmitted, it is required to track the vehicles for their identification. This is not feasible as most consumers will not like others to know about their personal identification. Therefore this has to come in balance and a tradeoff must be maintained between the authentication and privacy of the nodes.

*4) Network Scalability:*

The scale of the vehicular network in the world is exceeding continuously and as this number is growing, another problem is arising. Further, we know that there is no global authority to govern the standards for this network in the world.

*5) Incentives:*

Manufactures are interested to build applications that consumer likes most. Very few consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of VANET will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET.

Low tolerance for error: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause danger.

*6) Key Distribution:*

In VANETs, security mechanisms implemented reliant on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Keys distribution among vehicles is a major challenge in designing a security protocols.

## III. ATTACKS IN THE VANET

In order to get better protection from attackers, it is essential to have the knowledge about the attacks in VANET against security requirements. These attacks are based on

1) Identification and Authentication
2) Routing attack discussed below:

Attack on Identification and Authentication

### *A. Sybil:*

In this type of attack, a malicious vehicle claims to be at multiple locations with multiple identities thereby creating an illusion of traffic congestion. The malicious node can even spoil the proper functioning of the network by injecting false information.

### *B. Black Hole attack:*

In this attack, a malicious node pretends to have an optimum route for the destination node and indicates that packet should route through this node after transmitting the fake routing information. The impact of this attack is that the malicious node can either drop or misuse the intercepted packets without forwarding them.

### *C. Worm Hole attack:*

In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole.

It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunnelled packet arrive sooner than other packets transmitted over a normal multi-hop route.

### *D. Gray Hole attack:*

This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. It can be performed by three ways (i) malicious node may drop incoming packets while allow some packets to pass (ii) malicious node may behave as normal for some time and malicious for a certain time and (iii) malicious node may drop incoming packets from some specified nodes for some time and later on it behaves as a normal node. These different types of behavior make attack difficult to detect. Grayhole attack finally disrupts the network's performance by interfering with the route discovery process.

### *E. Denial of Service (DoS) Attack:*

can be done by the network insiders & outsiders. An insider attacker may jam the channel after transmitting dummy messages & thus, stops the network connection. An outsider attacker can launch a DoS attack by repeatedly disseminating forged messages with invalid signatures to consume the bandwidth or other resources of a targeted vehicle. The impact of this attack is that, VANET losses its ability to provide services to the legitimate vehicles.

Security is an important issue for routing in VANETs, because many applications will effect life-or-death decisions and illicit tampering can have devastating consequences. Security is an important issue for routing in VANETs, because many applications will effect life-or-death decisions and illicit tampering can have devastating consequences. The characteristics of VANETs make the secure routing problem more challenging and novel than it is in other communication networks. Another challenge related to routing is efficient data dissemination and data sharing in VANETs. Additional areas for improvement include the integration of privacy and security mechanisms into routing protocols and the establishment of priority routes for emergency and safety messages.

## IV. RELATED WORK

To provide secure VANET, many researchers present a set of solutions to solve different security problems which are discussed in this section.

Isaac, J.T.; Zeadally, S.; Camara, J.S. in [7] surveys the major security attacks and presents the corresponding countermeasures and cryptographic solutions.

Researchers in [13] – [16] dealt with routing protocols and gave effective solutions so that the

 

communication between the nodes is computational effective and leading to less congestion of network traffic.

Yong Hao, Yu Cheng, and Kui Ren in [17] proposed a solution of group formation combined with RSU is illustrated, which resulted in easy revocation of malicious vehicle, location privacy protection is improved and the system maintenance becomes flexible.

Wang, J., Yan, W in [18] suggested a new protocol for message checking, this protocol involves checking the Certificate Validity (CV) of the sender, the receiver of the message checks the CV of the message sender, the result of checking has three cases: in the first case, the receiver will consider the message if the sender has a valid certificate, second case occurs when the sender has invalid certificate, in this case the receiver will not regard the message, in the third case, the sender has not CV at all, the receiver will inform the RSU with the sender and check the received message, if it is correct the RSU will issue CV for the sender, otherwise it will issue invalid certificate and record vehicle's identity into the Certificate Revocation List (CRL).

To protect vehicular network against Sybil attacks, researchers B. Liu, B. Khorashadi, H. Du, D. Ghosal, C-N. Chuah and M. Zhang in [19] proposed a solution involves using on road radar, where each vehicle can see surrounding vehicles and receive reports of their GPS coordinates. By comparing what is seen to what has been heard, a vehicle can corroborate the real position of neighbors and isolate malicious vehicles.

Prabhakar, M.; Singh, J.N.; Mahadevan, G. in [20] proposed an essential complements to the passive mechanisms of encryption. For inputs as given security measures of the VANET, the defensive mechanism adopts game theoretic approaches and is comprised of three stages(i) uses heuristics based on ant colony optimization to identify known and unknown opponents (ii) Nash Equilibrium is employed for selecting the model for a given security problem and (iii) enables the defensive mechanism to evolve over traffic traces through the game theoretic model from the first stage.

### *A. Comparison*

After comparing the various research papers the drawbacks that are most common is high bandwidth consumption.
Secondly performance is low when we use the protocol in high traffic area. VANET node must confirm to hardware and bandwidth restriction. Lastly masquerading is possible.

## V. CONCLUSION

In this review paper we have compared various research papers on VANET to analyze the current drawbacks and objectives in the VANET research. With the wireless technology becoming pervasive and cheap, VANET is going to turn out to be the networking platform that would support the future vehicular applications. We laid out the several drawbacks including security and performance and several efforts are being undertaken to make VANET a reality. In future we would like to propose an algorithm that would enhance the performance with the maintenances of security using a light weight mechanism.

## REFERENCES

[1] F. Li, Y. Wang, "Routing in vehicular ad hoc networks: a survey, Veh. Technol. Mag.", IEEE 2 (2007) 12–22.
[2] S. Yousefi, et al., "Vehicular ad hoc networks (VANETs): challenges and perspectives", in: ITS Telecommunications Proceedings, 2006 6th International Conference on, 2006, pp. 761–766.
[3] I. Stojmenovic, J. Wu, Guest Editors' Introduction: Ad Hoc Networks, Computer 37 (2004) 0029–31.
[4] X. Sun, et al., Secure vehicular communications based on group signature and ID-based signature scheme, in: Communications, 2007. ICC'07. IEEE International Conference on, 2007, pp. 1539–1545.
[5] D. Jiang, L. Delgrossi, IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments, in: Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, 2008, pp. 2036–2040.
[6] P. Caballero-Gil, C. Hernández-Goya and A. Fúster-Sabater, "Securing Vehicular Ad-Hoc Networks", International Journal on Information Technologies & Security, vol. 1, (2009), pp. 25-36.
[7] J. T. Isaac, S. Zeadally and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks", Communications, IET, vol. 4, no. 7, (2010) April 30, pp. 894, 903.
[8] J. Fuentes, A. González-Tablas and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks", Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, (2010), pp. 894-911.
[9] A. Yusri Dak, S. Yahya and M. Kassim, "A Literature Survey on Security Challenges in VANETs", International Journal of Computer Theory and Engineering, vol. 4, no. 6, (2012) December, pp. 1007-1010.
[10] C. S. R. Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", PEARSON, ISBN 81-317-0688-5, (2011).
[11] M. S. Al-kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)", 6th IEEE International Conference on Signal Processing and Communication Systems (ICSPCS), (2012), pp. 1-9.
[12] I. Ahmed Sumra, I. Ahmad, H. Hasbullah and J. bin Ab Manan, "Classes of attacks in VANET", IEEE Saudi International in Electronics, Communications and Photonics Conference (SIECPC), (2011).
[13] F. Hui, "A survey on the characterization of Vehicular Ad Hoc Networks routing solutions ECS 257", Winter, (2005), pp. 1-15.
[14] J. Yin, T. El. Batt, G. Yeung and B. Ryu, "Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks", Proceeding of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, (2004), pp. 1-9.
[15] S. Y. Wang, "Predicting the Lifetime of Repairable Unicast Routing Paths in Vehicle-Formed Mobile Ad Hoc Networks on Highways", 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC), vol. 4, (2004), pp. 2815-2829.

 

[16] L. Briesemeister, A. G. DaimlerChrysler, Berlin, Germany and G. Hommel, "Role-Based Multicast in Highly Mobile but Sparsely Connected Ad Hoc Networks", First Annual Workshop on Mobile and Ad Hoc Networking and Computing, (MobiHOC), (2000), pp. 45-50.
[17] Y. Hao, Y. Cheng and K. Ren "Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs", IEEE GLOBECOM- 2008, pp. 4951-4955.
[18] J. Wang and W. Yan, "RBM: A role based mobility model for VANET", Proc. Int. Conf. Communications and Mobile Computing, vol. 2, (2009) January, pp. 437-443.
[19] B. Liu, B. Khorashadi, H. Du, D. Ghosal, C-N. Chuah and M. Zhang, "VGSim: An Integrated Networking and Microscopic Vehicular Mobility Simulation Platform", IEEE Communication Magazine Automotive Networking Series, vol. 47, no. 5, (2009) May, pp. 134-141.
[20] M. Prabhakar, J. N. Singh and G. Mahadevan, "Defensive mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization", IEEE International Conference on Computer Communication and Informatics (ICCCI), (2013) January, pp. 1-7

 